MASTER‘S THESIS ASSIGNMENT

I. Personal and study details

Student's name: **Endler Martin** Personal ID number: **483764**

Faculty / Institute: **Faculty of Electrical Engineering**

Department / Institute: **Department of Computer Science**

Study program: **Open Informatics**

Specialisation: **Cyber Security**

II. Master’s thesis details

Master’s thesis title in English:

FIDO2 USB Security Key

Master’s thesis title in Czech:

FIDO2 USB bezpečnostní klíč

Guidelines:

FIDO2 is a set of standards based on asymmetric cryptography that enables easy, secure, and phishing-resistant authentication.
The goal of this work is to create a new open-source implementation of a FIDO2 USB hardware external authenticator that is well-documented and thoroughly tested and offers a detailed yet accessible insight into the inner workings of FIDO2, which is something that existing implementations currently lack.
1. Make yourself familiar with the FIDO2 set of standards.
2. Review suitable technologies and existing similar projects.
3. Implement a working FIDO2 USB hardware external authenticator (“security key”) from scratch. External libraries can be used for some low-level generic components.
4. Follow software development best practices and use applicable software quality assurance methodologies.
5. Demonstrate the working of the implementation with authentication flows on real WebAuthn-enabled websites.
6. Document the work and make it publicly available on GitHub.

Bibliography / sources:

[1] W3C (April 8, 2021). Web Authentication: An API for accessing Public Key Credentials – Level 2. W3C Recommendation. https://www.w3.org/TR/webauthn-2/
[2] FIDO Alliance (June 21, 2022). Client to Authenticator Protocol (CTAP). CTAP 2.1 Proposed Standard. https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-errata-20220621.html
[3] USB Implementers Forum (April 27, 2000). USB 2.0 Specification. https://usb.org/document-library/usb-20-specification

